IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Greenbelt Division

LUTHER B. OAKES, M.D., individually and as representatives of the class, Plaintiff, vs. MARRIOTT INTERNATIONAL, INC., and STARWOOD HOTELS AND RESORTS WORLDWIDE, LLC, Defendants.	**Case No: _____** **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiff Luther B. Oakes, M.D. ("plaintiff" or "Oakes"), individually and on behalf of the class set forth below, brings the following class action complaint against defendants Marriott International, Inc. ("Marriott") and Starwood Hotels and Resorts Worldwide, LLC ("Starwood"):

PRELIMINARY STATEMENT

1. This case is about one of the largest data security breaches in history, affecting millions of consumers who have booked hotel reservations with the defendants, Marriott and Starwood.

2. As a result of this breach, plaintiff Oakes and the class members whose personal information was not safeguarded now face substantial risk of further injury from identity theft, credit and reputational injury, false tax claims, or even extortion.

3. On November 30, 2018, Marriott publicly acknowledged that it was subject to one of the largest data breaches in history.

4. The data security breach, which was ongoing over a period of four-years, disclosed the personal information of approximately 500 million hotel guests from Starwood's guest reservation database.

5. The information stolen in the breach includes names, mailing addresses, telephone numbers, email addresses, passport numbers, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences. For some, the information also included payment card numbers and payment card expiration dates.

6. Unbelievably, the defendants failed to detect the hackers' activities over the four-year period. As a result of the defendants' failure to protect its guests' sensitive information, Plaintiff Oakes and class members have been exposed to fraud, identity theft, and financial harm, as detailed below, and are subject to a heightened, imminent risk of such harm in the future.

7. Plaintiff Oakes seeks redress individually, and on behalf of those similarly-situated, for the injuries that he and class members sustained as a result of the defendants' negligent and intentional violations of law.

8. Plaintiff Oakes asserts these claims on behalf of a nationwide class of Marriott/Starwood guests for monetary relief, injunctive relief, corresponding declaratory relief, and other appropriate relief for Marriott's unlawful conduct, as described herein.

PARTIES

9. Plaintiff Oakes is a Mississippi citizen residing in Washington County, Mississippi. His personal information was compromised in the data breach after providing it to the defendants in connection with hotel stays at Marriott/Starwood properties.

10. Defendant Marriott is a global lodging and hospitality company with more than 6,700 properties across 130 countries and territories, reporting revenues greater than $22 billion in fiscal year 2017. Marriott maintains hotel brands including Marriott, Courtyard, Fairfield, and Ritz-Carlton, among others. Marriott is incorporated in Delaware, with its principal place of business in Bethesda, Maryland. Marriott may be served with process upon its registered agent, The

Corporation Trust Incorporated, 2405 York Road, Suite 201, Lutherville-Timonium, Maryland 21093-2264.

11. Defendant Starwood was acquired by Marriott in September 2016, and is Marriott's subsidiary. Starwood hotel brands include W, St. Regis, Sheraton, and Westin, among others. The Marriott-Starwood acquisition created the world's largest hotel conglomerate. Starwood is incorporated in Maryland, with its principal place of business in Stamford, Connecticut. Starwood may be served with process upon its registered agent The Corporation Trust Incorporated, 2405 York Road, Suite 201, Lutherville-Timonium, Maryland 21093-2264.

12. Upon information and belief, the defendants' wrongful acts and omissions leading to this data security breach occurred nationwide and in this district.

JURISDICTION & VENUE

13. This court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. Plaintiff Oakes, the class members, and the defendants are citizens of different states. There are more than 100 putative class members.

14. This court has personal jurisdiction over the defendants because Marriott maintains its principal place of business in Maryland, Starwood is incorporated in Maryland, and both companies regularly conduct business in Maryland and have sufficient minimum contacts in Maryland.

15. Venue is proper in this court pursuant to 28 U.S.C. § 1391(a) because Marriott's principal place of business is in this district and a substantial part of the events, acts, and omissions giving rise to the plaintiff's claims occurred in this district.

FACTS

16. On November 30, 2018, Marriott confirmed unauthorized access to its Starwood guest reservation database, which contained guest information relating to reservations at Starwood properties on or before September 10, 2018.

17. Marriott revealed that it first noticed irregular activity on September 8, 2018, after it received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database.

18. Marriott discovered that there had been unauthorized access to the Starwood network since 2014, and that an unauthorized party had copied and encrypted information, and took steps towards removing it – signaling that the information had been surreptitiously acquired by an unauthorized third party.

19. Despite learning of the massive data security breach on September 8, 2018, if not earlier, Marriott did not announce the breach for over two months until November 30, 2018. By waiting over 80 days to disclose the breach publicly, Marriott deprived its customers of an opportunity to take immediate precautions to protect themselves from identity theft and fraud.

20. Marriott acknowledges that the compromised database contains information on up to approximately 500 million guests who made a reservation at a Starwood property.

21. Marriott further acknowledged that for approximately 327 million guests, the information includes some combination of name, mailing address, telephone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates.

22. Affected persons are those who, like plaintiff Oakes, provided information to make reservations at a Starwood property[1], including Starwood Preferred Guest members and guests of Starwood branded timeshare properties.

[1] Starwood's properties include W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Meridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels.

23. The defendants have a history of inadequate data security practices. In November 2015, Starwood disclosed that point-of-sale systems at 54 of its hotels in North America were infected with malware, enabling unauthorized parties to access customers' payment data.

24. In February 2015, White Lodging Services Corporation – and independent hotel management company used by Marriott – confirmed a point-of-sale breach exposed customers' personal information and card data at 10 Marriott locations in the United States.

25. Additionally, the defendants were aware of numerous additional data hacks targeting the hospitality industry, including major hotel chains Hilton, Hyatt, Hard Rock, Four Seasons, Trump, Loews, Radisson, InterContinental, Omni, and Kimpton, among others.

26. Despite being a holder of sensitive personal information for millions of persons worldwide,[2] the defendants failed to prioritize data security by adopting reasonable safeguards to prevent and detect unauthorized access to its customer's

[2] In its privacy policy, Marriott acknowledges that its guests must provide their personal information in order to stay at a Marriott/Starwood property, and that Marriott seeks "to use reasonable organizational, technical and administrative measures to protect Personal Data." Marriott defines "Personal Data" as "data that identify you as an individual or relate to an identifiable individual." *See* Marriott Group Global Privacy Statement (last updated May 18, 2018), available at: https://www.marriott.com/about/privacy.mi.

information. The defendants had ample resources to prevent a breach, but failed to prioritize data security while spending millions on executive compensation, marketing, and other endeavors.

27. The defendants' conduct demonstrates a willful and conscious disregard for consumer privacy.

28. As a result of the defendants' conduct, plaintiff Oakes and the class members had their personal information exposed to sophisticated cyber-criminals who trade such information on an international black market.

29. Plaintiff Oakes and the class members are now at heightened risk for a variety of crimes, including but not limited to the following: tax fraud, identity theft such as opening fraudulent credit cards and loan accounts; various types of government fraud, such as obtaining a driver's license in the victim's name, or procuring government benefits with the victim's information; or medical fraud, such as using the victim's information to submit false insurance claims, illicitly obtain prescription drugs, etcetera.

30. In addition, plaintiff Oakes and the class members will have to deal with the repercussions of identity theft, which are time consuming and difficult to manage. These costs include not only theft of personal information, but costs associated with detection and prevention of identity theft and unauthorized use of

accounts, such as the purchase of credit monitoring or similar services. Other costs include but are not limited to: lower credit scores resulting from credit inquiries following fraudulent activities; costs associated with time spent and the loss of productivity from taking time to address and mitigate the actual and future consequences of the data breach, such as increased monitoring of accounts, and canceling and reissuing cards; costs associated with time spent obtaining credit freezes; costs associated with time spent obtaining fraud alerts on credit reports; re-issuing passports; canceling and re-issuing credit cards; canceling and re-issuing debit cards; and continued risk of expose to the thieves who now have, and can sell, the victims' information.

31. Plaintiff Oakes brings this action on his own behalf as well as on behalf of all similarly situated Marriott/Starwood customers.

32. Plaintiffs Oakes seeks declaratory and injunctive relief to prevent the defendants from continuing their unlawful conduct, and to recover damages and costs, including reasonable attorneys' fees, for the injuries that he and class members have sustained.

CLASS ACTION ALLEGATIONS

33. Plaintiff Oakes and the class members, as defined below, have been damaged by the defendants' negligent or reckless disregard for their personal

information, as well as the defendants' intentional silence for nearly 12 weeks regarding the existence and nature of the data security breach.

34. Plaintiff Oakes brings this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

35. Plaintiff Oakes asserts the claims herein on behalf of a proposed Nationwide Class ("the class") defined as follows:

> All United States residents whose information was made accessible in the data security breach announced by the defendants on November 30, 2018.[3]

36. Numerosity: The members of the class are so numerous that joinder of all class members is impracticable. More than 500 million Marriott/Starwood guests are affected by the data security breach.

37. Typicality: Plaintiff Oakes' claim is typical of other class members because, among other things, all class members were comparably injured by the defendants' negligent, reckless, and intentional conduct, as described above, which caused the data security breach.

[3] The following are excluded from the Nationwide Class: (1) the defendants, their offices and directors, as wells as their parent companies, subsidiaries and affiliates, legal representatives, and any co-conspirators; and (2) any judge or magistrate presiding over this action, and members of their families. The plaintiffs reserve the right to amend the class period and/or class definition if discovery and further investigation reveal that the class should be expanded, divided into additional subclasses, or modified in any way.

38. Adequacy: Plaintiff Oakes will fairly and adequately protect the interests of the class. Furthermore, he has retained counsel experienced in class actions and complex litigation.

39. Commonality and Predominance: Common questions of law and fact exist as to all class members and predominate over any questions solely affecting individual members of the class, including but not limited to:

a) whether the defendants owed duties under federal or state law to class members to protect their personal information, provide timely notice of unauthorized access to this information, and provide meaningful and fair redress;

b) whether the defendants breached said duties;

c) whether the defendants acted wrongfully by improperly monitoring, storing, and/or failing to properly safeguard the class members' personal information;

d) whether the defendants knew, or reasonably should have known, about the deficiencies in its data storage systems;

e) whether the defendants willfully failed to design, employ, and maintain a system adequate to protect consumers' personal information;

f) whether the defendants' representations regarding the security of its systems were false and misleading;

g) whether the defendants' acts and omissions violated applicable state consumer protection law;

h) whether the defendants' failures resulted in the data security breach at issue;

i) whether the defendants failed to properly and timely notify plaintiff Oakes and class members of the breach as soon as practicable after it was discovered;

j) whether the defendants' acts of concealment violated applicable state consumer protection laws; and

k) whether class members have been damaged and, if so, the appropriate relief.

40. This case is maintainable as a class action under Fed. R. Civ. P. 23(b)(2) because the defendants have acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

41. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(3) because questions of law and fact common to the class predominate over any

questions affecting only individual members of the class, and because a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

42. The defendants' conduct as described in this complaint stems from common and uniform policies and practices, resulting in a colossal data security breach as well as a deliberate and systematic delay strategy to hide the extent and nature of the breach from the very customers affected by the breach.

43. The class members do not have an interest in pursuing separate individual actions against the defendants, as the amount of each class member's individual claims are small compared to the expense and burden of individual prosecution.

44. Class certification also will obviate the need for unduly duplicative litigation that might result in inconsistent judgments concerning the defendants' practices. Moreover, management of this action as a class action will not present any likely difficulties. In the interests of justice and judicial efficiency, it would be desirable to concentrate the litigation of all class members' claims in a single forum.

45. Plaintiff Oakes intends to send notice to all class members to the extent required by Rule 23.

CLAIMS FOR RELIEF

COUNT I – NEGLIGENCE
(On behalf of the Nationwide Class)

46. Plaintiff Oakes, on behalf of the Nationwide Class, alleges and incorporates by reference the allegations paragraphs 1 through 45.

47. The defendants were, and continue to be, in a confidential, special, and/or fiduciary relationship with plaintiff Oakes and the class members by virtue of being trusted with their personal information.

48. At the very least, the defendants assumed a duty, and had duties imposed upon it by regulations, to comply with applicable security standards, regulations, and statutes, and to otherwise use reasonable care to safeguard plaintiff Oakes' and the class members' personal information.

49. The defendants also had a duty to timely inform plaintiff Oakes and the class members of the data security breach, and of the fact that their personal information had been compromised and/or stolen; furthermore, upon learning of the breach, the defendants had a duty to take immediate action to protect plaintiff Oakes and the class members from the foreseeable consequences of the breach.

50. By its acts and omissions as described herein, the defendants unlawfully breached their respective duties to plaintiff Oakes and the class members, who were harmed as a direct result.

51. The defendants knew, or should have known, that its system for processing and storing class members' personal information was replete with security vulnerabilities.

52. The defendants were negligent by continuing to accept, process, and store such information in light of its computer system vulnerabilities and the sensitivity of the personal information stored therein.

53. The data security breach, and resulting damages suffered by plaintiff Oakes and the class members, were the direct and proximate result of a number of actions and omissions, including but not limited to:

(a) the defendants' improper retention and storage of plaintiff Oakes' and class members' personal information;

(b) the defendants' failure to use reasonable care to implement and maintain appropriate security procedures reasonably designed to protect such information;

(c) the defendants' delay of nearly 12 weeks before notifying plaintiff Oakes and class members about the breach;

(d) the defendants' failure to take immediate and effective action to protect plaintiff Oakes and class members from potential and foreseeable damage.

54. The defendants' wrongful actions, as described above, reflect a breach of the duty of reasonable care and, therefore, constitute negligence.

55. Plaintiff Oakes and the class members have not in any way contributed to the data security breach or theft of their personal information.

COUNT II – NEGLIGENCE PER SE
(On behalf of the Nationwide Class)

56. Plaintiff Oakes, on behalf of the Nationwide Class, alleges and incorporates by reference the allegations in paragraphs 1 through 45.

57. Pursuant to the Graham-Leach-Bliley Act, 15 U.S.C. § 6801, the Federal Trade Commission Act, 15 U.S.C. § 45, and related state consumer data protection statutes, the defendants had a duty to protect and keep consumers' personal information secure, private, and confidential.

58. The defendants violated these laws by not adequately safeguarding plaintiff Oakes' and class members' personal information, as well as by not ensuring that the defendants themselves complied with applicable data security standards,

card association standards, regulations and/or statutes designed to protect such information.

59. The defendants' failure to comply with the Graham-Leach-Bliley Act, the Federal Trade Commission Act, industry standards, and state laws and regulations constitutes negligence *per se*.

COUNT III – BREACH OF FIDUCIARY DUTIES
(On behalf of the Nationwide Class)

60. Plaintiff Oakes, on behalf of the nationwide class, alleges and incorporates by reference the allegations in paragraphs 1 through 45.

61. The defendants, by virtue of its possession, custody, and/or control of plaintiff Oakes' and the class members' personal information, and the defendants' duty to properly monitor and safeguard said information, was, and continues to be, in a confidential, special, and/or fiduciary relationship with plaintiff Oakes' and the class members.

62. As a fiduciary, the defendants owed, and continue to owe, plaintiff Oakes and the class members:

(a) the commitment to deal fairly and honestly;

(b) the duties of good faith and undivided loyalty; and

(c) integrity of the strictest kind.

63. The defendants were, and continue to be, obligated to exercise the highest degree of care in carrying out the responsibilities to plaintiff Oakes and class members under such confidential, special, and/or fiduciary relationships.

64. The defendants breached their fiduciary duties to plaintiff Oakes and the class members when they failed to adequately store, monitor, and protect plaintiff Oakes' and class members' personal information.

65. The defendants willfully and wantonly breached their fiduciary duties to plaintiff Oakes and the class members or, at the very least, committed these breaches with conscious indifference and reckless disregard of plaintiff Oakes' and the class members' rights and interests.

COUNT IV – BREACH OF CONTRACT
(On behalf of the Nationwide Class)

66. Plaintiff Oakes, on behalf of the Nationwide Class, alleges and incorporates by reference the allegations in paragraphs 1 through 45.

67. Plaintiff Oakes and the class members were parties to actual or implied contracts with the defendants that required the defendants to properly safeguard their personal information from theft, compromise, and/or unauthorized disclosure.

68. Additionally, plaintiff Oakes and the class members were third-party beneficiaries to contracts between the defendants and other entities under which the

defendants are required to safeguard its customers' personal information from theft, compromise, and/or unauthorized disclosure.

69. The defendants' wrongful acts as described herein constitute breaches of these contracts.

COUNT V – BAILMENT
(On behalf of the Nationwide Class)

70. Plaintiff Oakes, on behalf of the Nationwide Class, alleges and incorporates by reference the allegations in paragraphs 1 through 45.

71. Plaintiff Oakes' and the class members' personal information is their property, which they delivered to the defendants for the sole and specific purpose of completing one or more commercial transactions.

72. The defendants accepted plaintiff Oakes' and class members' personal information and, thus, served as a bailees with respect to the above-referenced transaction(s).

73. The defendants, as bailees, owed a duty to plaintiff Oakes and class members and, in fact, had an express and/or implied contract with them to protect their personal information from theft, compromise, or unauthorized disclosure.

74. The defendants breached their duty and/or express and implied contracts with plaintiff Oakes and class members by improperly storing and

inadequately protecting their personal information from theft, compromise, and/or unauthorized disclosure, which directly and proximately caused plaintiff Oakes and class members to suffer damages.

75. The defendants' wrongful actions constitute breaches of their duties (and/or express and/or implied contracts) with plaintiff Oakes and the class members arising from the bailment.

COUNT VI – UNJUST ENRICHMENT
(On Behalf of the Nationwide Class)

76. Plaintiff Oakes, on behalf of the Nationwide Class, alleges and incorporates by reference the allegations in paragraphs 1 through 45.

77. Plaintiff Oakes brings this cause of action on behalf of the class members and, to the extent necessary, in the alternative to their breach of contract claims.

78. Plaintiff Oakes and the class members conferred a monetary benefit on the defendants in the form of money paid to the defendants for their services.

79. Plaintiff Oakes and the class members also provided their personal information to the defendants which the defendants utilized for monetary purposes.

80. The defendants appreciated or had knowledge of the benefits conferred upon them by plaintiff Oakes and the class members.

81. The money paid by plaintiff Oakes and the class members to the defendants should have been used by the defendants, in part, to pay for the costs of reasonable data privacy and security practices and procedures.

82. As a result of the defendants' conduct, plaintiff Oakes and the class members suffered actual damages in an amount equal to the difference in value between services with reasonable data privacy and security practices and procedures that the plaintiff and class members paid for, and inadequate services without reasonable data privacy and security practices and procedures that they received.

83. Under principles of equity and good conscience, the defendants should not be permitted to retain the money belonging to plaintiff Oakes and the class members because the defendants failed to implement adequate data privacy and security practices and procedures that the plaintiff and class members paid for.

84. The defendants should be compelled to disgorge into a common fund all unlawful or inequitable proceeds they received, and a constructive trust should be placed upon such funds for the benefit of plaintiff Oakes and the class members.

COUNT VII – VIOLATION OF MARYLAND PERSONAL INFORMATION PROTECTION ACT AND CONSUMER PROTECTION ACT
(On Behalf of the Nationwide Class)

85. Plaintiff Oakes, on behalf of the Nationwide Class, alleges and incorporates by reference the allegations in paragraphs 1 through 45.

86. The defendants are incorporated and/or headquartered in Maryland and are subject to the laws of Maryland. Pursuant to the Maryland Personal Information Protection Act (PIPA), Maryland Code, Commercial Law § 14-3501 *et seq.*, Maryland businesses have a statutory obligation to maintain the security of personal information of individuals.

87. As described herein, the defendants failed to implement and maintain reasonable security procedures and practices to protect the personal information of plaintiff Oakes and the class members, and thereby violated the PIPA, Maryland Code, Commercial Law § 14-3503(a).

88. The PIPA further provides that in the event of a security breach, notice must be given to consumers as soon as reasonably practicable following the investigation. The notice sent to the consumer must include: a description of the information compromised; contact information for the business, including a toll-free number if the business has one; toll-free numbers and addresses for each of the three credit reporting agencies: Equifax, Experian, and TransUnion; toll-free numbers, addresses, and websites for the Federal Trade Commission and the Office of Attorney General.[4]

[4] *See* Maryland Code, Commercial Law § 14-3504.

89. Prior to sending notification to consumers, the PIPA states that a business must notify the Office of the Attorney General that includes a brief description of the nature of the security breach, the number of Maryland residents being notified, what information has been compromised, and any steps the business is taking to restore the integrity of the system.[5]

90. As described above, the defendants did not timely notify affected individuals, including plaintiff Oakes and class members, that they were subject to a data breach.

91. The defendants' violations of the PIPA also constitute unfair or deceptive trade practices prohibited by the Maryland Consumer Protection Act ("MCPA"), and are subject to the MCPA's enforcement provisions.[6]

92. Accordingly, the defendants are liable to plaintiff Oakes and class members for damages and attorneys' fees under Maryland Code, Commercial Law § 13-408.

93. Plaintiff Oakes and the class members seek all remedies available under Maryland law including, but not limited to, damages and attorneys' fees.

[5] *Id.*
[6] *See* Maryland Code, Commercial Law § 14-3508.

PRAYER FOR RELIEF

94. As a direct and proximate cause of the defendants' wrongful conduct, plaintiff Oakes and the class members sustained, and will continue to incur, damages in the form of:

a) the unauthorized disclosure and/or compromise of their personal information;

b) monetary losses and damage to credit from fraudulent charges made upon their accounts; and

c) the burden and expense of credit monitoring.

95. Accordingly, plaintiff Oakes, individually and on behalf of the classes, requests relief as follows:

a) certification of the Nationwide Class pursuant to Fed. R. Civ. P. 23, as requested herein;

b) appointment of plaintiff Oakes as class representative, and the undersigned counsel as class counsel;

c) an order directing that reasonable notice of this action, as provided by Fed. R. Civ. P. 23(c)(2), be given to each and every class member;

d) equitable relief to prevent any additional harm including, but not limited to, provision of credit monitoring services for a period of time to be determined by a trier of fact;

e) an injunction permanently enjoining the defendants, as well as their subsidiaries and affiliates, from further engaging in the same acts or omissions that led to the data security breach described above;

f) a judgment in favor of plaintiff Oakes and class members under the legal theories alleged herein;

g) an award to the plaintiffs and class members of nominal damages, compensatory damages, and/or punitive damages, to the extent allowed by law;

h) an award to the plaintiffs and class members of restitution and/or disgorgement of profits;

i) an award of pre- and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of this complaint;

j) an award of reasonable attorneys' fees, costs, and expenses; and

k) granting such other relief as the court deems just and proper.

DEMAND FOR JURY TRIAL

96. Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, the plaintiff and the class demand a trial by jury.

Respectfully submitted December 4, 2018.

PAULSON & NACE, PLLC

/s/ Christopher T. Nace
Christopher T. Nace, Esq. #16442
1025 Thomas Jefferson St. NW
Suite 810
Washington, D.C. 20007
Phone: (202) 851-9899
Fax: (202) 223-6824
ctnace@paulsonandnace.com

BEASLEY, ALLEN, CROW, METHVIN, PORTIS & MILES, P.C.

/s/ W. Daniel "Dee" Miles, III
W. DANIEL "DEE" MILES, III*
ARCHIE I. GRUBB, II*
ANDREW E. BRASHIER*
LESLIE L. PESCIA*
218 Commerce Street
Montgomery, AL 36104
Tel: (334) 269-2343
Fax: (334) 954-7555
Dee.Miles@BeasleyAllen.com
Archie.Grubb@BeasleyAllen.com
Andrew.Brashier@BeasleyAllen.com
Leslie.Pescia@BeasleyAllen.com

C.W. WALKER, III
C.W. Walker III, LLC

/s/ C.W. "Bill" Walker, III
C. WILLIAM WALKER, III*
512 Main Street
Greenville, MS 38702
Tel: (662) 580-0070
Fax: (662) 550-4773
bill@bill-walker.com

** To be admitted pro hac vice*

SERVE DEFENDANTS AS FOLLOWS:

MARRIOTT INTERNATIONAL, INC.
The Corporation Trust Incorporated
2405 York Road, Suite 201,
Lutherville-Timonium, Maryland 21093-2264

STARWOOD HOTELS & RESORTS WORLDWIDE, LLC
The Corporation Trust Incorporated
2405 York Road, Suite 201,
Lutherville-Timonium, Maryland 21093-2264